No. 18-55169

In The

United States Court of Appeals for the Ninth Circuit

James E. Andrews,

Plaintiff-Appellant,

v.

Sirius XM Radio Inc.,

Defendant-Appellee.

Appeal from the United States District Court
for the Southern District of California
No. 5:17-cv-01724 (Hon. Percy Anderson)

Brief of Sirius XM Radio Inc.

Thomas Demitrack
JONES DAY
901 Lakeside Ave.
Cleveland, OH 44114
Tel: (216) 586-3939
Fax: (216) 579-0212

Shay Dvoretzky
Jeffrey R. Johnson
JONES DAY
51 Louisiana Ave., N.W.
Washington D.C. 20001
Tel: (202) 879-3939
Fax: (202) 626-1700

Counsel for Defendant-Appellee Sirius XM Radio Inc.
(additional counsel on inside cover)

Lee A. Armstrong
JONES DAY
250 Vesey Street
New York, New York 10281
Tel: (212) 326-3939
Fax: (212) 755-7306

CORPORATE DISCLOSURE STATEMENT

Defendant-Appellee Sirius XM Radio Inc. submits the following corporate disclosure statement pursuant Federal Rule of Appellate Procedure 26.1. The undersigned, counsel of record for Sirius XM, certifies:

1. Sirius XM Radio Inc. is a wholly-owned subsidiary of Sirius XM Holdings Inc., a publicly-held corporation.

2. As of July 11, 2018, Liberty Media Corporation, a publicly-held corporation, owned, directly or indirectly, approximately 71% of the outstanding common stock of Sirius XM Holdings Inc.

3. To the best of Sirius XM's knowledge, no other person, entity, or group owns 5% or more of the outstanding common stock of Sirius XM Holdings Inc.

Dated: July 11, 2018

JONES DAY

/*s*/ Shay Dvoretzky

Counsel for Defendant-Appellee Sirius XM Radio Inc.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

TABLE OF AUTHORITIES
(continued)

Page(s)

OTHER AUTHORITIES

INTRODUCTION

When James Andrews purchased a used car from Auto Source, he showed the dealer his driver's license and helped the dealer fill out Form 262, the Vehicle/Vessel Transfer and Reassignment Form that must ultimately be filed with the California DMV. And because Andrews' car came equipped with a subscription to Sirius XM's satellite radio service, Sirius XM—through an intermediary and pursuant to an agreement between it and Auto Source—obtained Andrews' contact information and mailed him letters about that subscription.

Andrews asserts that, because Sirius XM allegedly obtained his personal information from his driver's license and Form 262, this humdrum sequence of events constituted a *federal crime* under the Drivers Privacy Protection Act of 1994. If Andrews were correct, a wide swath of innocent conduct—such as mailing a hotel guest to fill out a survey after he provided his driver's license for identification, or getting an address from a friend's driver's license when shipping a surprise gift—would be unlawful.

Andrews is mistaken. As the district court and many other courts have recognized, the DPPA "regulates the disclosure of personal information contained in the records of state motor vehicle departments," *Reno* v. *Condon*, 528 U.S. 141, 143 (2000); it does not restrict the use of information provided by the customer himself, even if the customer conveyed it through a driver's license. And neither Andrews' driver's license nor the dealer's version of Form 262 qualifies as a "motor vehicle record" under the DPPA's definition. The decision below should be affirmed.

JURISDICTIONAL STATEMENT

The district court had jurisdiction over Andrews' federal claims under 28 U.S.C. § 1331. It granted Sirius XM summary judgment on January 9, 2018, disposing of all of Andrews' claims in a final judgment. ER 3–4. Andrews timely noticed an appeal on February 7, 2018. ER 1–2. This Court has jurisdiction under 28 U.S.C. § 1291.

ISSUES PRESENTED

I. Whether the district court erred in concluding that Sirius XM did not violate the DPPA when it acquired personal information that Andrews himself provided to Auto Source.

II. Whether the district court abused its discretion in denying Andrews leave to add a claim under the Computer Fraud and Abuse Act, where his only claimed "loss" was his purported inability to sell his own information.

STATEMENT OF THE CASE

A. Sirius XM Works with Dealerships To Provide Trial Subscriptions to Purchasers of Pre-Owned Automobiles

Sirius XM provides the nation's only satellite radio service. Through its Pre-Owned Program, Sirius XM works with thousands of car dealerships across the country to provide subscriptions to Sirius XM's satellite radio service to customers who purchase pre-owned vehicles equipped with Sirius XM-compatible radios. ER 271 (Berger Decl. ¶ 2). Sirius XM offers valuable subscriptions to dealers' customers. In return, dealers who participate in the Pre-Owned Program agree to (1) explain Sirius XM's services to their customers; and (2) provide Sirius XM with the names and addresses of those who purchase Sirius XM-compatible cars, along with the Vehicle

Identification Numbers of those cars. *Id.* Sirius XM uses that information to activate the customers' subscriptions. It also contacts them to explain Sirius XM's satellite radio service and ask them if they wish to continue with that service once their trial period has ended.

Auto Source, a car dealership in Banning, California, signed up for the Pre-Owned Program in October 2015 through its Dealer Management System (DMS), a piece of software provided by AutoManager, Inc. In its enrollment form, Auto Source acknowledged that Sirius XM "requires the use of data that exists in [its] [DMS], including customer data, to activate [its] customers' SiriusXM trial service and to communicate with customers regarding their Trial Subscriptions and options to extend their SiriusXM services following the Trial Subscriptions." SER 8 (Exh. A to Berger Decl.). It therefore "agree[d] to share with SiriusXM … [its] DMS data on an on-going basis." *Id.* It also agreed to "take all necessary action required to facilitate such sharing of data with SiriusXM," including authorizing AutoManager "to extract and share [its] DMS data with SiriusXM." *Id.* Under Sirius XM's agreement with AutoManager, AutoManager promised to "deliver to Sirius XM" "on a daily basis" "used vehicle sales transaction data for Sirius XM Enabled Vehicles," including "Dealer IDs, VINs and Customer Information." SER 17 (Exh. B to Berger Decl.).

B. Sirius XM Received Andrews' Contact Information After He Bought a Sirius XM-Equipped Pre-Owned Car from Auto Source

Plaintiff James Andrews purchased a pre-owned 2012 Chevy Equinox from Auto Source on January 14, 2017. ER 283 (Compl. ¶ 16); *see* ER 169 (Pltf.'s Opposing Statement of Fact ¶ 2) (explaining that the sale took place on January 14, not January 15, as the complaint alleged). At the time of his purchase, Andrews orally provided his street address to Auto Source. ER 224 (Andrews Decl. in Opposition ¶ 6). Andrews also provided Auto Source with his name and P.O. Box address, though he claims he provided this information by showing Auto Source his driver's license rather than by stating his name or P.O. Box address out loud. *Id.* Finally, Andrews provided his telephone number, street address, P.O. Box, and name to Auto Source in filling out Form 262, "Vehicle/Vessel Transfer and Reassignment Form," a multipurpose California form that serves as an odometer disclosure, bill of sale, and power of attorney. ER 190 (Form 262); ER 224–25 (Andrews Decl. in Opposition ¶¶ 3–6).

Andrews' Chevy Equinox came equipped with a Sirius XM radio. Accordingly, pursuant to Auto Source's enrollment agreement, Auto Source (through its AutoManager DMS) provided Sirius XM with a sold record about Andrews' pre-owned vehicle on January 14, 2017. ER 272 (Berger Decl. ¶ 5). That record contained information taken from the sales contract between Auto Source and Andrews, including his name and street address. ER 269 (Carpenter Decl. ¶ 7). Sirius XM did not, however, obtain Andrews' P.O. Box from that source. Sirius XM got that information through

Epsilon, a contractor which used the U.S. Postal Service's National Change of Address database to provide Sirius XM with Andrew's P.O. Box number on January 16, 2017. *Id.* (Carpenter Decl. ¶¶ 8, 11). Around the same time, Sirius XM activated the subscription covering Andrews' automobile. *Id.* (Carpenter Decl. ¶ 6).

C. Sirius XM Contacted Andrews, So He Sued

Between January 2017 and August 2017, Sirius XM sent letters to Andrews at his P.O. Box address, including letters encouraging him to resume Sirius XM service after his subscription expired. ER 283 (Compl. ¶ 18); ER 287 (letter). Sirius XM also called him to see whether he wished to sign up for a paid subscription. ER 284 (Compl. ¶ 20).

In response, Andrews filed a putative class action against Sirius XM for alleged violations of the Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq.* ER 279–86. He apparently believed that Sirius XM acquired his contact information from the California Department of Motor Vehicles. *E.g.*, ER 284 (Compl. ¶ 21) (alleging that Sirius XM "obtained [his] name and address, as well as his phone number, from the motor vehicle records, most likely the registration documents submitted to the DMV after he purchased the car"); ER 284–85 (Compl. ¶ 24) (alleging that Sirius XM "used personal information from motor vehicle records to mail similar letters and make similar phone calls to the class members"). He sought statutory damages of $2,500 per violation and an injunction prohibiting Sirius XM from "illegally obtain[ing] and us[ing] personal information from motor vehicle records to solicit car owners." ER 285, 286 (Compl. ¶ 27, Prayer for Relief 4).

Sirius XM tried to explain to Andrews and his counsel that Auto Source and Epsilon, not the DMV, had provided Sirius XM with his information. ER 5–7 (Op. 1–3). Andrews' counsel then confirmed Sirius XM's account through his own investigation. Glen Bohannan, Auto Source's service manager, stated that he met with a Sirius XM representative in October 2015. ER 235 (Bohannan Decl. ¶ 4). He also admitted that his email address was used to sign up for Sirius XM's Pre-Owned Program. ER 235 (Bohannan Decl. ¶ 3). Finally, he admitted that, while he did not "believe" that he had "visited some website" to sign up for the program, "[m]aybe the salesman" gave him his "tablet or laptop" and "asked [him] to click somewhere on the screen." ER 235–36 (Bohannan Decl. ¶ 6). And although Auto Source's president and owner insisted that Sirius XM somehow "lied to and tricked Mr. Bohannan" into signing up for a program whose terms authorized AutoManager to share Auto Source's customers' information with Sirius XM, he acknowledged that Bohannan's testimony showed "what happened here." ER 231 (Mukerjee Decl. ¶¶ 15, 16).

D. The District Court Granted Summary Judgment to Sirius XM Because Neither It Nor AutoManager Obtained Andrews' Information from DMV Records

Nevertheless, Andrews persisted. He argued that Sirius XM violated the DPPA by "us[ing] … information obtained from the driver['s] license [he] provided to Auto Source and the information Auto Source input into AutoManager to prepare and submit" Form 262. ER 7 (Op. 3).

The district court disagreed. "[T]he DPPA 'regulates the disclosure of personal information contained in the records of state motor vehicle departments,'" as well as "'the resale and redisclosure of drivers' personal information by private persons who have obtained that information from a state DMV.'" ER 7–8 (Op. 3–4) (quoting *Reno* v. *Condon*, 528 U.S. 141, 143, 146 (2000)). In addition to criminal fines, the statute provides that anyone "who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under [the DPPA] shall be [civilly] liable to the individual to whom the information pertains." 18 U.S.C. § 2724(a).

Under these provisions, Sirius XM "did not obtain [Andrew's] 'personal information' from a 'motor vehicle record' 'contained in the records' of the DMV." ER 8 (Op. 4) (quoting *Reno*, 528 U.S. at 143). "Like the Supreme Court and the vast majority of other courts to have analyzed the issue," the district court "interpret[ed] the DPPA's definition of 'motor vehicle record' as requiring that the DMV be the source of the 'record.'" ER 8 (Op. 4) (collecting cases). Under that approach, neither Andrews' driver's license, nor the information he provided to prepare Form 262, nor Form 262 itself qualified, as none of them were *DMV* records at the time Auto Source transmitted them to Sirius XM through AutoManager. ER 9 (Op. 5).

Similarly, though a driver's license contains information that is also contained in the records of the DMV, it is "not itself" a "motor vehicle record." ER 9 (Op. 5). That term covers "any record that *pertains to* a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor

vehicles." 18 U.S.C. § 2725(1) (emphasis added). To qualify as a "motor vehicle record," then, a driver's license would have to "pertain to" itself, which is nonsense. ER 9 (Op. 5). Moreover, "strange and far-reaching results" would "follow" from Andrews' proposed interpretation. ER 9 (Op. 5). For instance, Andrews' reasoning "would criminalize the conduct of, and create civil liability for, the Good Samaritan who finds a lost wallet and uses the name and address found on the driver['s] license … to return the wallet to its owner." ER 9–10 (Op. 5–6). "Acknowledging that a driver['s] license is not itself a 'motor vehicle record'" avoids that "absurd" result. ER 10 (Op. 6).

The district court also denied Andrews' request for leave to amend his complaint to add a claim under the Computer Fraud and Abuse Act. The CFAA makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] … information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). It also allows those who "suffer[] damage or loss by reason of a violation of this section" to seek damages. *Id.* § 1030(g). Andrews wished to amend his complaint to add a claim that Sirius XM violated these provisions by using "'back door' access" through "some sort of arrangement" it had with AutoManager to acquire customer information without Auto Source's knowledge or consent. ER 11 (Op. 7).

The district court found that it would have been "futile" to allow Andrews to add this claim. ER 12 (Op. 8). As relevant here, such an action may be brought only if the violation caused "loss to 1 or more persons … aggregating at least $5,000 in value." ER 11 (Op. 7) (incorporating certain factors listed in § 1030(c)(4)(A)(i)). But Andrews'

claimed loss—the loss of his and other putative class members' ability to sell their personal information for marketing purposes—does not qualify as a "loss" under the CFAA. "[I]t is not a 'reasonable cost' he incurred in 'responding to an offense' or 'restoring the data, program, system, or information to its condition prior to the offense.'" ER 12 (Op. 8) (quoting 18 U.S.C. § 1030(e)(11) (defining loss)). Nor is it "revenue lost, cost incurred, or other consequential damages incurred because of an interruption of service." *Id.* (quoting 18 U.S.C. § 1030(e)(11)). "Subsequent economic damage unrelated to the computer itself does not constitute 'loss'" under this provision, *id.* (quoting *New Show Studios LLC v. Needle*, 2014 WL 2988271, at *7 (C.D. Cal. Jun. 30, 2014)); otherwise, the CFAA would be "transform[ed] … from an anti-hacking statute into an expansive misappropriation statute," *id.* (quoting *United States* v. *Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) (en banc)).[1]

SUMMARY OF ARGUMENT

I. Sirius XM did not violate the DPPA by allegedly acquiring Andrews' contact information from his driver's license or Form 262.

A. In the 1980s and early 1990s, state DMVs across the country engaged in the troubling practice of selling or freely disclosing the personal information in the DMV's files to third parties. This practice, which often took place without drivers' consent or

[1] Andrews also unsuccessfully sought leave to amend to add a claim under the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ER 13 (Op. 9). He has not appealed that decision.

even knowledge, had serious repercussions: several people were murdered when stalkers or ex-spouses obtained their address from the DMV, while many more faced an onslaught of random solicitations when companies purchased entire databases of contact information. Congress responded with the DPPA, whose every provision focuses on the unlawful acquisition of personal information from the DMV's records.

B. Sirius XM did not violate the DPPA when it allegedly obtained Andrews' information from his driver's license and from Form 262.

Take first Andrews' driver's license. The DPPA defines a "motor vehicle record" as "any record that pertains to a motor vehicle operator's permit … or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Under this definition, to qualify as a "motor vehicle record," a driver's license would have to "pertain to" itself, which is absurd. Moreover, even if a driver's license qualified as a "motor vehicle record," Sirius XM could not be held liable for information allegedly derived from it. As its text, legislative history, and a welter of case law establish, the DPPA is only concerned with information obtained (directly or indirectly) from the DMV; it does not regulate the use of information disclosed by a consumer himself, even if he happens to disclose it via his driver's license. Indeed, on Andrews' theory, a hotel that mailed a survey to those who use their driver's licenses to provide their contact information when checking in would be liable. It would be absurd to read the DPPA—which creates both criminal and civil liability—so broadly.

Andrews' claims about Form 262 fare no better. The yet-to-be-filed version of Form 262 prepared by Auto Source was not a "motor vehicle record" under the DPPA. As both common usage and the Privacy Act (the model for the DPPA) establish, a "record" is an official document maintained by a government agency, not a piece of paper that happens to contain the same information that will ultimately find itself in the DMV's files. And even if Auto Source had already filed Form 262 when Sirius XM's agent allegedly obtained information from it, Sirius XM would still not be liable because, again, the DPPA protects only against the disclosure of information ultimately tracing to the DMV's files, not to someone else's disclosure.

C. Andrews' counterarguments are meritless. *First*, he spends much of his brief debating whether the information in question must come directly from the DMV. But neither Sirius XM nor the district court have insisted that only those who ask the DMV for information are potentially liable. Instead, Sirius XM argued (and the district court held) that the information must ultimately *trace to* a request for information to the DMV, whether or not there are intermediaries involved afterward. Andrews does not meaningfully challenge that proposition, which resolves this case because neither Sirius XM, nor AutoManager, nor Auto Source ever requested any information about Andrews from the California DMV.

Second, Andrews tries to explain how a driver's license might "pertain to" itself, but is ultimately forced to rewrite the statute, conceding that it "could have been written clearer" if Congress had wanted to enact his version of the law. Br. 38. He also argues

that there are policy reasons for treating driver's licenses as "motor vehicle records," but none of his examples—such as a stalker who orders a duplicative driver's license, Br. 39—support his wildly expansive view of the Act.

Third, Andrews tries to explain away the absurd consequences of his view, insisting that many apparent violators (such as the Good Samaritan who returns a license or the spouse who makes an order using one) might be excused under doctrines such as consent or necessity. But for starters, it is strange to believe that Congress subjected a wide range of innocent (or even laudable) behavior to prima facie liability, subject to the vagaries of implied federal common law defenses. It is also far from clear that many of these defenses would save these would-be violators from liability: the DPPA places strict limits on the scope of acceptable consent; Good Samaritan laws themselves often have narrow confines; and many situations—such as the hotel that mails a survey to the address found on the guest's voluntarily provided driver's license—do not seem to qualify for any of Andrews' exceptions.

Fourth, Andrews tries to support his position with a smattering of district court decisions. Most of these non-binding authorities do not suggest that Sirius XM could be held liable in these circumstances, and the one that might is badly reasoned, heavily criticized, and contrary to the great weight of authority.

II. The district court properly denied Andrews' request for leave to add a CFAA claim to his complaint, because that request was futile.

A. To have a civil cause of action under the CFAA, Andrews must allege a "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). The statute defines a "loss" as "any reasonable cost to any victim," "includ[ing]" the "cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense," as well as "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11).

Andrews' alleged loss—the loss of his and his fellow class members' purported chance to sell their contact information to Sirius XM—does not qualify under this provision. *First*, Andrews' claimed loss is a claim of "revenue lost," but he does not (and could not) argue that his lost revenue stems from an "interruption of service." Because the statute specifically includes that requirement when addressing lost revenue claims, a host of canons of statutory construction—the canon against superfluity, the specific governs the general, and noscitur a sociis—prohibit him from trying to sneak his claim into the "any reasonable cost" category. *Second*, this Court has often insisted that the CFAA should not be transformed from an anti-hacking statute into an expansive misappropriation provision, and Andrews' claim would do just that.

B. Andrews does not meaningfully address the text of the CFAA, instead asserting that *Creative Computing* v. *Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004),

already resolved this issue in his favor. That is not true. *Creative Computing* did not address what *counts* as a loss, because it was undisputed that the victim spent more than $5,000 in remedial measures tied directly to the computer breach. Instead, *Creative Computing* simply held that plaintiffs need not show any particular intrusion cost them $5,000 in losses. And even if this Court decided to examine Andrews' two other cases (both district court decisions), they would not support his claim. One addressed the irrelevant issue of whether the statute covered more than just physical damage, while the other simply asserted Andrews' position without reasoning or support.

C. Even if missed marketing opportunities qualify as "losses" within the CFAA, Andrews could not credibly plead a violation. It is simply implausible to think that he and his fellow class members could have sold their information to Sirius XM for *$50*, the amount he would have to allege to qualify. In addition, Andrews cannot and has not plead the other facts required to make his claim plausible: that there is a market for this information, that he has tried to or would try to participate in that market, and that his fellow class members would do likewise.

STANDARD OF REVIEW

This Court reviews the district court's grant of summary judgment de novo. *See Gordon* v. *County of Orange*, 888 F.3d 1118, 1122 (9th Cir. 2018). It reviews the district court's decision to deny leave to amend for an abuse of discretion. *Rentmeester* v. *Nike, Inc.*, 883 F.3d 1111, 1125 (9th Cir. 2018).

ARGUMENT

I. SIRIUS XM DID NOT VIOLATE THE DPPA BY ALLEGEDLY ACQUIRING ANDREWS' INFORMATION FROM HIS DRIVER'S LICENSE AND FORM 262

A. In the DPPA, Congress Responded to State DMVs' Unauthorized Disclosure of Personal Information

In 1989, a stalker shot the young actress Rebecca Schaeffer to death in the doorway of her Los Angeles apartment building. She had done everything she could to keep trouble away; both her home phone number and address were unlisted. But her assailant—an obsessed fan—easily tracked her down. He simply hired a private investigator, who in turn got her address from the California DMV just by asking. *See* 140 Cong. Rec. H2518-01, 1994 WL 140035 (Apr. 20, 1994) (statement of Rep. Moran); Statement of Congressman James P. Moran Before the Subcommittee on Civil and Constitutional Rights on H.R. 3365, 1994 WL 212698 (Feb. 4, 1994).

Rebecca Schaeffer was not the only one hurt by the ready availability of information contained within the files of state DMVs. A New Mexico woman who moved three times to escape her abusive husband was found murdered in his car after he took down her friend's car's license plate number, "went to the department of motor

vehicles," and retrieved her friend's address "for a nominal fee." Testimony of David Beatty, Director of Public Affairs for the National Victim Center, Before the House Subcommittee on Civil and Constitutional Rights, 1994 WL 212822 (Feb. 3, 1994). Iowa teenagers wrote down the license plate numbers on expensive cars, took the information to the DMV to request the owners' addresses, and subsequently burglarized their homes. *See* 139 Cong. Rec. S15745-01, S15761 (Nov. 16, 1993) (statement of Sen. Boxer). And a woman who unsuccessfully tried to *save* her pregnancy received letters condemning her for "having killed [her] own child" after activists jotted down her license plate number near the clinic she visited, secured her "name and address from department of transportation records," and decided that she must have gone to the clinic to get an abortion. 139 Cong. Rec. S15766 (Nov. 16, 1993) (statement of Sen. Harkin). In each of these (and many other) incidents, perfect strangers acquired sensitive personal data—name, address, height, weight, and so on—simply because, "[u]nder the law in over 30 States, it [was] permissible to give out to any person [that information] if a drivers' license or vehicle plate number [was] provided to a state agency." 139 Cong. Rec. S15765 (Nov. 16, 1993) (statement of Sen. Biden).

"Concerned that personal information collected by States in the licensing of motor vehicle drivers was being released—even sold—with resulting loss of privacy for many persons," *Maracich* v. *Spears*, 570 U.S. 48, 51–52 (2013), Congress responded with the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721–25. In keeping with its origins,

the DPPA "regulates the disclosure of personal information contained in the records of state motor vehicle departments." *Reno*, 528 U.S. at 143.

Its provisions repeatedly reflect this focus on a state's own records. The DPPA's key substantive prohibition—titled "Prohibition on release and use of certain personal information from State motor vehicle records"—bars a DMV and its employees from "knowingly disclos[ing] or otherwise mak[ing] available … personal information … about any individual obtained by the department in connection with a motor vehicle record" except as provided by the rest of the statute. 18 U.S.C. § 2721(a)(1).[2] In § 2721(b), the DPPA spells out the circumstances under which a DMV or its employees may or must disclose such information. For example, DMVs or their employees must disclose such information "in connection with matters of motor vehicle driving or safety," and may disclose it "[f]or use by any government agency … in carrying out its functions," "[f]or any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains," or "[f]or use by any requester, if the requester

[2] "'[P]ersonal information' means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3).

A "motor vehicle record" is "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." *Id.* § 2725(1).

demonstrates it has obtained the written consent of the individual to whom the information pertains." *Id.* § 2721(b)(1), (b)(11), (b)(13).

Section 2722 then turns to those who seek information from DMV files, making it unlawful "knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b)" and to "make false representation to obtain any personal information from an individual's motor vehicle record." Section 2723 makes clear that Congress takes violations by public officials and private parties seriously by subjecting those who "knowingly violate[]" the DPPA to a criminal fine, *id.* § 2723(a), with state DMVs subject to "civil penalty … of not more than $5,000 a day" if they have "a policy or practice of substantial noncompliance," *id.* § 2723(b). Finally, the DPPA provides a cause of action for those whose information is unlawfully handed over: "[a] person who knowingly obtains, discloses, or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains" in a "civil action," where the court "may award" (among other things) "actual damages, but not less than liquidated damages in the amount of $2,500." *Id.* § 2724(a), (b)(1).

B. Sirius XM Did Not Violate the DPPA When It Acquired Information That Andrews Himself Disclosed

Andrews admits that neither Sirius XM nor anyone else requested his information from the California DMV. See Br. 4, 6 (admitting that Auto Source got Andrews' information from Andrews himself when he purchased his car and that

"Sirius [XM] apparently obtained Andrews' information from Auto Source"). Andrews insists, however, that Sirius XM violated the DPPA: He provided his driver's license and either filled out (or provided the information used to fill out) Form 262 when he purchased his automobile from Auto Source, and Sirius XM (through AutoManager) obtained his personal information from those documents. Br. 19–20.

If Andrews were right, the DPPA would subject an enormous swath of ordinary conduct to criminal and civil liability. Imagine you check into a hotel and hand over your driver's license when the clerk asks for your contact information. If the hotel later mails you a survey asking about your stay, it has committed a crime, and you may sue it for $2,500. Or imagine you find someone's driver's license in the road and mail it back to them. Andrews admits that, on his view of the statute, you are liable—again, both criminally and civilly—unless you can persuade the court to apply some sort of unwritten affirmative defense. Br. 41–44.

That is not the law. Under the DPPA as properly construed, Sirius XM did not "obtain[]" Andrews' "personal information[] from a motor vehicle record" when it allegedly acquired information from his self-disclosed driver's license and Form 262.

1. A driver's license is not a "motor vehicle record" for purposes of the DPPA

The DPPA defines a "motor vehicle record" as "any record that *pertains to* a motor vehicle operator's permit … or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1) (emphasis added). But a driver's license cannot

qualify under that definition. Viewing a driver's license itself as a "record that pertains to a motor vehicle operator's permit … or identification card" would "render the definition's use of both 'record' and 'pertains to' … surplusage because the driver['s] license would be 'pertaining' to itself." ER 9 (Op. 5); *see also, e.g.*, *Whitaker v. Appriss, Inc.*, 266 F. Supp. 3d 1103, 1108 (N.D. Ind. 2017) ("A driver's license isn't a part, member, accessory, or product of a motor vehicle operator's permit; it *is* a motor vehicle operator's permit." (emphasis in original)). That makes no linguistic sense.

2. The DPPA does not cover information ultimately obtained from consumers themselves, even if that information is conveyed through a driver's license

Even if Andrews' driver's license qualified as a "motor vehicle record," Sirius XM still would not be liable for obtaining any information derived from that license. The DPPA covers only the acquisition of information through methods that ultimately track back to the DMV's files. But Sirius XM did not acquire Andrews' information that way. Instead, it acquired Andrews' information when he voluntarily provided his driver's license to Auto Source.

Every aspect of the DPPA shows that it was concerned with information ultimately obtained from the state DMV, not information independently provided by consumers themselves. Its title is "Prohibition on Release and Use of Certain Personal Information *from State Motor Vehicle Records*." 18 U.S.C. ch. 123 (emphasis added). Its chief substantive prohibition governs the disclosure of information by "[a] State department of motor vehicles" or its "officer[s], employee[s], or contractor[s]." *Id.*

§ 2721(a). And its other provisions all key back to this principle limitation. Section 2721(b)'s list of "[p]ermissible uses" outlines the scenarios in which personal information "shall" or "may be disclosed" by DMV personnel. *See also, e.g.*, *id.* § 2721(b)(11) (for any use "in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains"); *id.* § 2721(d) (allowing states to set up a mechanism to inform people of "request[s] for personal information" and to seek a "[w]aiver" of their right to have that information withheld). Indeed, the DPPA provision at issue here—section 2724(a)'s "[c]ause of action"—does not purport to create any new rights against acquisition or disclosure, but rather creates civil liability where someone "knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter." *Id.* § 2724(a) (emphasis added).

The DPPA's legislative history also demonstrates that Congress meant only to restrict the dissemination of personal information ultimately housed within a DMV's files, not to prohibit people from obtaining or using information that others themselves disclose. Congress enacted the DPPA for two main reasons: to address "a growing threat from stalkers and criminals who could acquire personal information from state DMVs," and to stem "the States' common practice of selling personal information" for commercial gain. *Maracich*, 133 S. Ct. at 2198; *see supra* 15–18. Both reasons have everything to do with disclosure that ultimately traces to the DMV's own records, and

nothing to do with disclosure of information that also (and independently) happens to be found within DMV records.

A contrary view of the statute is impossible to square with the DPPA's legislative history. To Sirius XM's knowledge, not *one* senator, congressperson, or witness at a congressional hearing ever suggested that the DPPA prohibited the disclosure of information originally contained somewhere besides a DMV's files. Instead, every example provided in support of the legislation—Rebecca Schaeffer's murder, the teenagers who robbed the homes of luxury car owners, the domestic violence victims tracked down by their estranged spouses, and on and on—involved a situation in which someone requested and obtained material from the DMV. Moreover, when congresspersons like Senator Biden explained that the DMV closed the loophole in the "law in over 30 States" that made it permissible for DMVs "to give out" a person's information, 139 Cong. Rec. S15765 (Nov. 16, 1993), they could not have had a contrary interpretation of the statute in mind. The laws in question authorized *state DMVs* to disclose personal information; they said nothing about whether parties could disclose information that happened to be provided to them via a driver's license by the license holder himself.

Not surprisingly, then, virtually every court to consider the question has concluded that the DPPA does not prohibit the disclosure of information ultimately obtained from a source other than the DMV, even if that information happened to be delivered via a driver's license. In *Fontanez* v. *Skepple*, for example, Fontanez presented

her driver's license as identification when visiting her boyfriend in prison, and one of the prison guards then allegedly used that information to send her "flowers and a teddy bear" as her "new admirer." 563 F. App'x 847, 848 (2d Cir. 2014). While that conduct was "surely inappropriate," it did not violate the DPPA because the information "was not obtained from a search of DMV records by a DMV employee or authorized DMV reseller." *Id.* at 848, 849; *see id.*at 849 ("[T]he statute was intended to bar the State from disclosing personal information obtained from DMV records without the individual's consent," not to cover "every misuse of information on a driver's license voluntarily provided as proof of identity.").

Siegler v. *Best Buy Co. of Minn., Inc.*, 519 F. App'x 604 (11th Cir. 2013) (per curiam), reached the same result. Siegler sued after Best Buy scanned the magnetic strip on the driver's license he presented when he returned a computer mouse. The Eleventh Circuit rejected his claim: "A plain reading of the DPPA makes clear that the Act was intended to prohibit only the disclosure or redisclosure of information *originating* from state department of motor vehicle … records." *Id.* at 605 (emphasis in original); *see also id.* ("On its face, the Act is concerned only with information disclosed, in the first instance, by state DMVs."). The vast majority of district courts agree. *See, e.g.*, *O'Brien* v. *Quad Six, Inc.*, 219 F. Supp. 2d 933 (N.D. Ill. 2002) (no liability where defendant videotaped presentation of driver's license and shared the information on it with another nightclub); *Whitaker*, 266 F. Supp. 3d at 1108–10 (no liability where defendant sold personal information from accident records prepared with information derived

from driver's licenses given to officers at the scene); *Hurst* v. *State Farm Mut. Auto. Ins. Co.*, 2012 WL 426018, at *10 (D. Del. Feb. 9, 2012) (no liability where defendant "obtains th[e] information directly from the plaintiff"); *Ocasio* v. *Riverbay Corp.*, 2007 WL 1771770, at *1 (S.D.N.Y. June 19, 2007) (no liability where defendant obtained the information from employment records that included a copy of the plaintiff's driver's license); *Figueroa* v. *Taylor*, 2006 WL 3022966, at *3–4 (S.D.N.Y. Oct. 23, 2006) (no liability where defendant obtained the information from employment records that included the plaintiff's learner's permit).

It could hardly be otherwise; if the DPPA covered the use of information obtained from somewhere other than the DMV's own files, it would be absurdly broad. For example, if Andrews is right, then "a person who uses information on her spouse's driver's license … to make an order" would be *criminally* liable for that conduct, as well as civilly liable "to the spouse for a DPPA violation." *Whitaker*, 266 F. Supp. 3d at 1109. After all, the spouse would have "knowingly obtain[ed], disclose[d], [and] use[d] personal information, from a motor vehicle record, for a purpose not permitted under [the DPPA]" on Andrews' reading of the statute. 18 U.S.C. § 2724(a). So too for the district court's proposed hypothetical—a Good Samaritan who found someone's wallet and used the name and address on her driver's license to return it. ER 9–10 (Op. 5–6). And so, too, for many other hypotheticals. Consider, for instance, the hotel mentioned above that sends a follow-up survey to an address it obtained when a guest used his driver's license to convey that information at check-in rather than write out the address

for the clerk. Or consider the interested person who looks up the docket *in this case* and, using Andrews' partially redacted driver's license (which Andrews himself placed in the record), reaches out to him with questions. ER 189 (driver's license). Under Andrews' view, that person has violated the DPPA's criminal and civil provisions.

Courts "will not construe a statute in a manner that leads" to such "absurd" results in any case, *Nixon* v. *Missouri Municipal League*, 541 U.S. 125, 138 (2004), but it would be particularly inappropriate to do so here. The DPPA's civil cause of action mirrors its criminal prohibitions. *Compare, e.g.*, 18 U.S.C. § 2723 (anyone who "knowingly violates this chapter shall be fined under this title"), *with id.* § 2724(a) (providing a civil cause of action against anyone who "knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter"). Because the relevant parts of the DPPA have both "criminal and noncriminal applications," the "rule of lenity applies" in interpreting any ambiguity in its scope. *Leocal* v. *Ashcroft*, 543 U.S. 1, 11 n.8 (2004). At the very least, it is ambiguous whether the DPPA makes everyone who has ever returned a lost wallet or helped a spouse make a reservation criminally liable. Sirius XM's interpretation must be correct.

3. Sirius XM cannot be held liable even if a driver's license is a motor vehicle record from the DMV because Andrews himself was an "authorized recipient" of that information

Finally, even if Andrews' driver's license might somehow "pertain to" itself and thus qualify as a "motor vehicle record," and even if obtaining information from it qualifies because Andrews himself got the license from the DMV, Sirius XM still could

not be held liable. In that scenario, Andrews would qualify as an authorized recipient under § 2725(b)(11), which allows the DMV to disclose "[f]or any … use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains." 18 U.S.C. § 2721(b)(11). "An authorized recipient under subsection (b)(11)," however, "may … redisclose personal information for any purpose." *Id.* § 2721(c) (emphasis added). By providing his driver's license to Auto Source, Andrews did just that. Sirius XM cannot be held civilly liable—let alone criminally liable, as Andrews' arguments entail—because he chose to hand over his driver's license when buying a car.

4. Form 262 does not fall within the DPPA either

Andrews also asserts that Sirius XM violated the DPPA because it obtained some of his personal information from Form 262, which Auto Source completed (using information that he provided) as part of his purchase of an automobile. Br. 14, 19. Like his argument about his driver's license, however, this claim fails because Form 262 was not a "motor vehicle record" and because Sirius XM did not acquire any information on it "from" the California DMV.

First, the yet-to-be-filed version of Form 262 prepared by Auto Source from which Sirius XM allegedly received Andrews' information was not a "motor vehicle record" under the DPPA. In legal usage, a "record" isn't just any old piece of paper that happens to contain information. Instead, a "record" is something official—"an authentic official copy of a document … deposited in keeping of officer designated by

law," Black's Law Dictionary (6th ed. 1990); "an official writing recording facts or events," The New Webster's Comprehensive Diction of the English Language (deluxe ed. 1985); or "[a]n account officially written and kept as evidence or testimony," Webster's II New Riverside University Dictionary (1984). To qualify as a "motor vehicle record," then, a document must be found within—or at least have originated from—the DMV's official files. After all, the DMV is the office "designated by law" with the task of "keeping" driving-related information, so if personal information is to come "from a motor vehicle record," it must derive from something that was once officially maintained by the DMV.

This interpretation of "motor vehicle record" aligns with common English usage. If someone walked into a car dealership with a handwritten card setting forth his proposed trade-in's make, model, mileage, and Vehicle Identification Number, no one would say that he had produced a "motor vehicle record," even if all of that same information might ultimately end up in the DMV's files on an official form. Sirius XM's understanding of "motor vehicle record" also accords with the Privacy Act of 1974, 5 U.S.C. § 552a, which served as a model for the DPPA. *See, e.g.*, Statement of Congressman James P. Moran Before the Subcommittee on Civil and Constitutional Rights on H.R. 3365, 1994 WL 212698 (Feb. 4, 1994) ("The bill incorporates … the intent of the 1974 Privacy Act."); 139 Cong. Rec. S15764 (Nov. 16, 1993) (statement of Sen. Boxer) (same). The Privacy Act governs the collection and dissemination of information about individuals by federal agencies, and it defines a "record" just as Sirius

XM does: an "item, collection, or grouping of information about an individual *that is maintained by an agency*." 5 U.S.C. § 552a(a)(4) (emphasis added).

Under this understanding of "motor vehicle record," the version of Form 262 at issue here does not qualify. Andrews has pointed to no evidence in the record to suggest that the "change of ownership form [was] actually transmitted to the DMV" before Sirius XM allegedly retrieved information from it. ER 9 (Op. 5). At that time, then, Form 262 had exactly the same status as any other self-prepared but unfiled document that might ultimately receive government approval: it was not "an authentic *official* copy of a document … *deposited* in keeping of officer designated by law," "an *official* writing recording facts or events," or "[a]n account *officially* written and kept as evidence or testimony." Thus, even if Form 262 might have ultimately *become* a government record once the DMV accepted it for filing and maintained it within the DMV's own records, Sirius XM cannot be held liable for any information acquired from it before that time.

Second, even if there were some dispute about whether the DMV had received Form 262 at the time Sirius XM allegedly acquired information from it,[3] that dispute

[3] Andrews asserts without explanation that "the DMV form 262 might have been accessed by Sirius after it was transmitted to the DMV" and that this "factual uncertainty" precludes summary judgment. Br. 14, 19. But this argument is forfeited, as it made no appearance in Andrews' briefing before the district court. In any event, to survive summary judgment, Andrews had to provide evidence suggesting that Sirius XM (or someone else who later gave the information to Sirius XM) obtained Form 262 from the DMV after it was transmitted to the DMV. Andrews points to no such information in the record.

would be immaterial because Sirius XM still would not have acquired information "from" a motor vehicle record in that scenario. As explained above, the DPPA only covers situations in which the DMV itself ultimately disclosed the information to someone, not when the consumer himself provides information that happens to find itself within a government record. *See supra* 20–24.

On this point, too, the Privacy Act is instructive. Much like the DPPA, the Privacy Act generally bars agencies from "disclos[ing] any record which is contained in a system of records by any means of communication … except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." 5 U.S.C. § 552a(b). In applying this provision, courts have "uniformly recognized" the "distinction between information retrieved from a system of records and information independently acquired." *Thomas* v. *Dep't of Energy*, 719 F.2d 342, 345 (10th Cir. 1983). In keeping with this principle, courts have refused to find violations stemming from the dissemination of "information obtained independently of any records, … *even if identical information is contained in the records*." *Wilborn v. HHS*, 49 F.3d 597, 600 (9th Cir. 1995) (emphasis added), *abrogated in part on other grounds by Doe* v. *Chao*, 540 U.S. 614, 618 (2004); *see also*, *e.g.*, *Doyle* v. *Behan*, 670 F.2d 535, 539 (5th Cir. 1982) (rejecting liability because the information was drawn, not "from a system of agency records," but from the discloser's "independent knowledge"); *Thomas*, 719 F.2d at 346 (rejecting liability where the information was acquired "through [the discloser's] participation in discussions with supervisory personnel" even if the discloser "knew or

should have known" the same information "may have existed in the Department's system of records as well"). Because there is no evidence to suggest that either Sirius XM or AutoManager ever acquired Form 262 from the California DMV, Sirius XM cannot be held liable even if Andrews could prove that Form 262 was transmitted to and accepted by the California DMV before the time AutoManager allegedly accessed it.

C. Andrews' Challenges to the District Court's Decision Are Meritless

Despite all of this, Andrews insists that Sirius XM (and myriad others) can be held criminally liable for using information obtained from driver's licenses and unfiled forms that a consumer himself turns over. None of his counterarguments in support of that breathtaking position have merit.

1. Andrews apparently does not dispute that the information in question must have originated with the DMV

Andrews begins his attempted rebuttal by mischaracterizing the district court's and Sirius XM's position. He insists, over and again, that on our view, "the DPPA only prohibits a person from obtaining information directly from the DMV." Br. 20–21; *see also id.* at 21 (contending that the DPPA does not just prohibit the acquisition or use of information "*that was obtained directly from the department of motor vehicles*" (emphasis in original)); *id.* at 22 (contending that the DPPA "does not require that the personal information have come from the DMV itself or that the motor vehicle record … be in the possession of the DMV at the time the defendant obtained the personal information"); *id.* at 25 (contending that "[a] citizen suffers the same harm" whether

the personal information "contained in motor vehicle records is transmitted directly from the DMV to a marketing company as he would if the information were transmitted from motor vehicle records to one company and then retransmitted to the defendant").

Sirius XM never argued, and the district court never held, that Sirius XM must have obtained personal information directly from the DMV to violate the statute. Instead, the district court held that the DMV "must be the source of the 'record'" from which the information ultimately derives. ER 8 (Op. 4); *see also id.* ("[T]he Act was intended to prohibit only the disclosure *or redisclosure* of information *originating* from state [DMV] records." (second emphasis in original)). With that understanding, most of Andrews' critique dissolves. For instance, as Andrews points out, the statute's scienter requirement would make little sense if the DPPA covered only those who directly acquired information from the DMV, as they would always know they are requesting information from motor vehicle records. Br. 22. But Sirius XM agrees that parties may be held liable if they knowingly obtain personal information derived from *others'* requests to the DMV, so this supposed criticism does not affect its position.

Andrews' brief is curiously silent about the position the district court in fact adopted. Indeed, at times he seems to accept that the information in question must have originated from DMV records. *E.g.*, Br. 29 (contending that information from the driver's license qualifies because the license "was ultimately issued by the DMV, so the original source of the information would be the DMV"). If so, then Andrews' DPPA claim must fail. Neither Auto Source nor Sirius XM ever queried the state department

of motor vehicles for Andrews' information. Instead, Andrews himself provided his own information, both orally and by handing over his driver's license and providing the information used to fill out Form 262. Because Andrews himself indisputably provided Auto Source with his information, that information did not come "from a motor vehicle record" for purposes of the DPPA.

2. Andrews cannot explain how an unfiled form or his driver's license qualifies as "motor vehicle record" under the statute

Andrews also tries to prove that, even if the DPPA covers only information originally derived from the DMV's files, his claim may proceed because both Form 262 and his driver's license are "motor vehicle records" from the DMV. Br. 37–39. He is mistaken.

Take first Form 262. Andrews seems to acknowledge that, to qualify as a "motor vehicle record," his Form 262 must have at least been filed with the DMV when Sirius XM allegedly obtained information from it through AutoManager and Auto Source. Br. 19. But that isn't enough for Sirius XM to be liable.[4] Instead, there must be credible evidence that Auto Manager obtained the information *from the DMV based on the filed version of the form*. Andrews has never pointed to any evidence, because there is none. Accordingly, Andrews' attempt to rely on Form 262 to support his DPPA claim must fail.

[4] For this reason, the alleged disputed facts surrounding the time at which Form 262 reached the DMV, *see* Br. 11–12, were immaterial to Sirius XM's motion for summary judgment.

Andrews' attempt to rely on his driver's license fares just as poorly. As explained, a "motor vehicle record" is "any record that pertains to a motor vehicle operator's permit … or identification card." *See supra* 19–20. And as explained, a driver's license can hardly "pertain[] to" itself, so it cannot count as a "motor vehicle record."

Andrews halfheartedly tries to counter this textual argument, insisting first that "[i]f you delete the 'pertains to' language then nothing is left to be a motor vehicle record." Br. 38. It is unclear why he makes this point; it is *Andrews*, not Sirius XM or the district court, who wants to read "pertains to" out of the statute by treating a driver's license as a record that "pertains to" itself. Andrews next asserts that "[a]dding the 'pertains to' language does not rule out a driver's license from being a motor vehicle record, but instead uses that as an example while expanding the universe of records subject to the DPPA." Br. 38. But that claim simply repeats Andrews' conclusion; it does not explain how that conclusion is textually defensible. Indeed, Andrews ultimately all but gives up on that attempt. He admits that the statutory definition "could have been written clearer" if Congress had actually meant to adopt his view, for instance by defining a "motor vehicle record" as "any record *including or pertaining to* a motor vehicle operator's permit … or identification card." Br. 38 (emphasis in original); *see also id.* (claiming that the DPPA is "not ambiguous nor are the words 'record' and 'pertains to' superfluous even if they are partially redundant). Of course, "it is for Congress, not this Court, to rewrite the statute." *Blount* v. *Rizzi*, 400 U.S. 410, 419 (1971).

Andrews also provides a policy rationale for revising the DPPA as he would: unless a driver's license counts as a motor vehicle record, a stalker who "obtained a person's home address from a DMV printout containing the same information" would be liable, but not one who "simply … order[ed] a duplicative driver license from the DMV." Br. 39. Congress had a reason for drawing this supposedly irrational line: treating a driver's license as a "motor vehicle record" in Andrews' fashion might vastly increase the scope of the statute, whereas treating a DMV printout as one could not possibly do so. Indeed, insofar as Congress was worried about the remote possibility of someone falsely obtaining information from the DMV in the fashion Andrews proposes, it enacted a *different* provision of the DPPA to handle the problem: under 18 U.S.C. § 2722(b), it is unlawful "to make false representation to obtain personal information from an individual's motor vehicle record," *id.*, as a stalker would certainly have to do to "order a duplicate driver license," Br. 39. In other words, there is no need—and no justification—for rewriting the definition of "motor vehicle record" as Andrews would.

3. Andrews cannot avoid the absurd consequences of his view

Andrews also unsuccessfully tries to explain away the bizarre results that follow from his interpretation of the DPPA. For instance, he *accepts* that, under his understanding of the statute itself, a Good Samaritan—one who finds a driver's license and uses the contact information on it to return it to its holder—would be liable. Br. 41. He asserts, however, that because "Good Samaritans are exempt from liability for

numerous acts that would otherwise be treated as criminal or civil violations," they must be immune from the DPPA penalties that Andrews' view would otherwise impose on them: a criminal fine and $2,500 in statutory damages. Br. 41.

Andrews cannot so easily escape from this all-too-real hypothetical. Andrews cites no authority for his proposition that Good Samaritans are generally immune, and, in fact, Good Samaritan immunity is often quite limited. In California, for instance, the primary Good Samaritan statute protects only those who "render[] emergency care at the scene of an emergency," Cal. Bus. & Prof'l Code § 2395, not everyone who does the right thing. Similarly, insofar as other Good Samaritans might receive their protection through doctrines such as implied consent—like the person whose battery is excused because he is performing mouth-to-mouth resuscitation or the Heimlich maneuver, *see* Br. 41—those who return driver's licenses would not be so fortunate under the DPPA. Every time it mentions consent, it requires proof beyond implication. *See, e.g.*, 18 U.S.C. § 2721(b)(11) (allowing disclosure for any purpose if the state has obtained the person's "express consent"); *id.* § 2721(b)(13) (similar if the requester has obtained the person's "written consent"); *id.* § 2725(5) (defining "express consent" to mean "consent in writing"). Andrews does not explain how courts could use implicit consent to save Good Samaritans when the DPPA itself requires more.

Of course, the Good Samaritan isn't the only one that faces criminal liability for ordinary actions under Andrews' view of the statute; according to him, the DPPA also makes it illegal to use a spouse's driver's license information to make a purchase, as well

as to access the district court docket *in this case*, which contains a partially redacted image of his driver's license. Br. 43–44. Here, too, Andrews tries to rely on consent to escape these absurd results: "presumably the spouse acted with consent in using information from the driver license to make a purchase," Br. 43–44, and Andrews himself "waived any privacy expectations" when he "consented to publication of his driver license," Br. 44. As just explained, however, implicit or presumed consent such as that between spouses—or between litigants and the public—generally does not suffice under the DPPA. And if Andrews is correct that he waived his DPPA rights—as to *any* use by *any* third party—by putting his driver's license on the docket, then he's just given his case away. After all, he also gave his driver's license to Auto Source. Why didn't that similarly waive his supposed DPPA rights as to any use by any third party?

Andrews also tries to combat the district court's interpretation with some supposedly absurd hypotheticals of his own—a spouse who "stole his wife's driver license to make a purchase for himself" and a robber who "stole [Andrews'] wallet so [the robber] could have [a] look at his driver license to discover his address." Br. 44. It is true that, on the district court's and Sirius XM's view of the statute, there is no *DPPA* liability in such scenarios, because driver's licenses do not qualify as "motor vehicle records." But that is hardly absurd. The DPPA was not designed to remedy every misuse of personal information that happened to come from a driver's license; instead, it responded to the "growing threat from stalkers and criminals who could acquire personal information *from state DMVs*" and "*the States'* [then-]common practice of

selling personal information to businesses engaged in direct marketing and solicitation." *Maracich*, 570 U.S. at 57 (emphasis added). Considering that context, it is hardly surprising that Congress chose not to make every driver's-license-related incident a federal crime, especially when doing so would also render countless ordinary activities unlawful.

4. Andrews cannot identify any well-reasoned decisions supporting his position

Finally, Andrews tries to support his capacious interpretation of the DPPA with a few citations, but even the sparse, non-binding authority he identifies does not help his case. Take first *Wilcox* v. *Bastiste*, 2017 WL 2525309 (E.D. Wash. June 9, 2017). There, the Washington State Patrol sold collision reports containing personal information to third parties. The Patrol admitted that "the personal information [it used when filling out accident reports] *[wa]s obtained from DMV records* and upload[ed] into a software program that the WSP troopers use to compose the collision reports." 2017 WL 2525309, at *1 (emphasis added). In granting a preliminary injunction, the court rejected the argument that the DPPA's protections "do not apply to [personal] information [from motor vehicle records] when that information is conveyed to a third party." *Id.* at *2. As explained above, neither Sirius XM nor the district court have advanced that argument. *See supra* 30–32. Instead, as also explained above, that's just not this case: Sirius XM obtained the information at issue from Andrews' voluntarily provided driver's license and the then-unfiled Form 262, not from any motor vehicle

record originally within the DMV's possession. *Wilcox* has no relevance in that scenario, because the Patrol *conceded* that it pulled DMV files to complete the forms.

The identical companion cases of *Garey* v. *Farrin*, 2017 WL 4357445 (M.D.N.C. Sept. 29, 2017), and *Hatch* v. *Demayo*, 2017 WL 4357447 (M.D.N.C. Sept. 29, 2017), do not help Andrews' claim either. The plaintiffs there alleged that the defendant law firms obtained their personal information from accident reports compiled in violation of the DPPA. The court rejected the argument that the DPPA "only regulates the disclosure of information held by a state DMV." *Garey*, 2017 WL 4357445, at *8. Insofar as the court meant to suggest that the DPPA covered the situation here—liability for information from a driver's license or an unfiled form—its statement was pure dicta: the complaint alleged that the information came "from a department of motor vehicles, either from [a] driver's license *or from the database of drivers' license data maintained by*" the North Carolina Division of Motor Vehicles. *Id.* at *1 (emphasis added). Moreover, that dicta was of the worst sort: the court's one-paragraph analysis did not acknowledge the DPPA's history, the welter of contrary case law interpreting it, or the absurd consequences that would follow from the court's broad interpretation.

So too for *Moncier* v. *Harris*: while the court stated without analysis that a driver's license was a "motor vehicle record" for purposes of Tennessee's equivalent statute, it did so only in the course of holding that the state could *redact* information when responding to open records requests because it did not know "whether personal information contained in the seizure records was obtained from unprotected source

materials, *i.e.*, a source other than a motor vehicle record or a protected database." 2018 WL 1640072, at *8 (Tenn. Ct. App. Apr. 5, 2018). If anything, *Moncier*'s focus on the source of the information supports Sirius XM's view of the statute, not Andrews'.

That leaves Andrews' "leading case," Br. 33—the criticized district court decision in *Pavone* v. *Law Offices of Anthony Mancini, Ltd.*, 205 F. Supp. 3d 961 (N.D. Ill. 2016). There, the plaintiff alleged that the defendant attorney obtained his personal information from an accident report prepared by state troopers. The court acknowledged that the information in question ultimately had to come from the DMV: "'[I]f the original source of the … information is the state department of motor vehicles, the DPPA protects the information throughout its travels.'" *Id.* at 964 (quoting *Whitaker v. Appriss, Inc.*, 2014 WL 4536559, at *4 (N.D. Ind. Sept. 11, 2014). It held, however, that "information obtained from a driver's license *is* information obtained from a motor vehicle record," because "[a] driver's license number and the other information contained on a driver's license is, without question, 'part' of a motor vehicle operator's permit." *Id.* at 966 (emphasis in original).

Pavone cannot support the weight that Andrews puts on it. First, because *Pavone* recognized that the information must ultimately come from a motor vehicle record, it eliminates Andrews' claim insofar as it is premised on Form 262, which AutoManager accessed from Auto Source's files, not the DMV's. Second, its conclusion that a driver's license is itself a motor vehicle record badly misread the DPPA. Again, the statute prohibits knowingly obtaining "personal information" from a "motor vehicle record,"

defined as a "record that *pertains to* a motor vehicle operator's permit … or identification card." 18 U.S.C. § 2725(1). As *Whitaker* explained, for a viable claim, there should be, "separately, 'personal information,' a 'record,' and a 'motor vehicle operator's permit'" (or identification card). 266 F. Supp. 3d at 1109. But on *Pavone*'s view, there isn't: there is either a driver's license that somehow "pertains to" itself, or the *information* on the driver's license is wrongly treated as both "record" and "personal information." *See id.* Finally, *Pavone* did not address any of the consequences of its view, consequences that render the DPPA absurdly broad.

Andrews' sparse cases provide no reason to depart from the overwhelming authority on point. The DPPA is not violated when someone acquires personal information from the plaintiff when he himself hands over his driver's license or helps fill out part of an unfiled form.

II. THE DISTRICT COURT PROPERLY DENIED ANDREWS' FUTILE REQUEST TO ADD A CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT

Andrews also insists that the district court should have allowed him to press his claim that Sirius XM violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, through the supposed "'back door' access" that allowed AutoManager to access Auto Source's dealer management software "without Auto Source knowing this was happening and without any involvement by Auto Source in the process." ER 11 (Op. 7). The district court did not abuse its discretion in denying leave to raise this meritless claim.

A. Andrews Cannot Plausibly Allege "Loss" Within the Meaning of the CFAA

The CFAA makes it a crime to "intentionally access[] a computer without authorization or [to] exceed[] authorized access[] and thereby obtain[] … information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). "Any person who suffers damage or loss by reason of a violation" of this provision "may maintain a civil action against the violator," so long as "the conduct involves 1 of the factors" set forth in the first five subsections of section 1030(c)(4)(A)(i). *Id.* § 1030(g). The only factor under which Andrews purported to bring his claim, ER 94 (Proposed Amended Compl. ¶ 38)—and the only one even potentially relevant here—is whether the offense caused "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." *Id.* § 1030(c)(4)(A)(i)(I). Whether Andrews could have brought a viable CFAA claim turns on whether Andrews could plausibly allege a qualifying loss.[5]

He cannot. The CFAA defines "loss" as "any reasonable cost to any victim," but then lists specific costs that it "include[s]," such as the "cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense," as well as "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

[5] Of course, given the evidence showing that Sirius XM secured Auto Source's permission for AutoManager to access and send along its customers' data, Andrews' claim also fails because Sirius XM never accessed a computer without or beyond authorization.

Id. § 1030(e)(11). Under this carefully articulated scheme, Andrews' purported loss—the profits he and his fellow class members could have received by somehow selling their contact information to Sirius XM on their own—cannot qualify as a "reasonable cost," because that loss did not stem from any "interruption of service."

That result flows from the strongest canons of statutory construction. Consider first the "commonplace of statutory construction that the specific governs the general." *Morales* v. *Trans World Airlines, Inc.*, 504 U.S. 374, 384 (1992). Although the "general/specific canon is perhaps most frequently applied to statutes in which a general permission or prohibition is contradicted by a specific prohibition or permission," it also "has full application" where "a general authorization and a more limited, specific authorization exist side-by-side." *RadLAX Gateway Hotel, LLC* v. *Amalgamated Bank*, 566 U.S. 639, 645 (2012). In such situations, the "terms of the specific authorization must be complied with"; otherwise, the specific authorization would be "swallowed by the general" one, violating *another* "cardinal rule" of statutory construction, namely the canon against "superfluity." *Id.*

RadLAX illustrates these principles nicely. There, the Bankruptcy Code deemed a bankruptcy plan's treatment of a secured creditor's claims to be "fair and equitable" if it met any of three conditions: if "the secured creditor retain[ed] its lien … and receive[d] deferred cash payments"; if the property was sold "free and clear of the lien" at an auction at which the creditor could bid with the amount owed to it to increase the purchase price; or if the creditor received the "indubitable equivalent" of its claims. *Id.*

at 643–44. A debtor tried to discharge a lien after an auction at which the secured creditor was *not* allowed to credit bid, contending that the creditor still received the "indubitable equivalent" of that lien. *See id.* at 642–43. The Supreme Court rebuffed the attempt: the credit-bidding clause was a "detailed provision that spell[ed] out the requirements for selling collateral free of liens," trumping the "broadly worded" indubitable-equivalent provision that "sa[id] nothing about such a sale." *Id.* at 646.

So too here. Andrews claims "revenue lost"—the money that he and other putative class members could have made had they been able to sell their information to Sirius XM. But the statutory definition contains a clause dealing directly with "revenue lost," and it requires that loss to occur "because of interruption of service"—a qualification Andrews cannot possibly meet. If Andrews' lost profits could nonetheless qualify as a "reasonable cost," then the statute's detailed discussion of revenue lost would be superfluous, and its specific provisions would be overridden by its general one. That is not how the CFAA should be read. *See Brown Jordan Int'l, Inc.* v. *Carmicle*, 846 F.3d 1167, 1174 (11th Cir. 2017) (the statute distinguishes between "the direct costs of responding to the violation" and "consequential damages resulting from interruption of service"); *Yoder & Frey Auctioneers, Inc.* v. *EquipmentFacts, LLC*, 774 F.3d 1065, 1074 (6th Cir. 2014) ("[T]he plain language of the [CFAA] treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an 'interruption in service.'"); *Nexans Wires S.A.* v. *Sark-USA, Inc.*, 166 F. App'x 559, 562–63 (2d Cir. 2006) (no "loss" where former employees misappropriated confidential

proprietary information to form a competing company because "no interruption of service occurred").

There are other, independent reasons not to treat missed marketing opportunities as a "reasonable cost" under the CFAA. This Court has stressed that the CFAA is an "anti-hacking statute," not an "expansive misappropriation statute." *United States* v. *Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) (en banc). For instance, the two examples of "reasonable cost[s]" provided in the definition reflect the CFAA's limited focus on harms directly caused by the computer intrusion itself: the first covers the costs of "responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense," while the second (as explained above) covers only consequential damages sustained "because of interruption in service." 18 U.S.C. § 1030(e)(11). Because "a general statutory term should be understood in light of the specific terms that surround it," *Hughey* v. *United States*, 495 U.S. 411, 419 (1990), "reasonable cost" should therefore be understood to include only the direct harms stemming from a computer breach, not downwind consequences far removed from the scope of the risk presented by hacking.

The other factors that give rise to a private cause of action under the CFAA—unauthorized access that alters the course of someone's medical treatment, that causes "physical injury" to someone, that "threat[ens] … public health or safety," or that "damage[s]" a government computer used "in furtherance of the administration of justice, national defense, or national security," 18 U.S.C. § 1030(c)(4)(A)—further

illustrate that Congress had much more serious cases in mind than Andrews' supposed desire to sell the information about his vehicle purchase himself. So too does the rule of lenity. Like the DPPA, the CFAA is a *criminal* statute whose private right of action is inextricably intertwined with its punitive provisions, thereby requiring that any ambiguity be construed in favor of civil (and therefore potentially criminal) defendants. *See supra* 25.

It is no wonder, then, that many courts have recognized that "[p]urely economic harm unrelated to the computer impairment or computer damages is not covered" by the CFAA's definition. *Custom Packaging Supply, Inc.* v. *Phillips*, 2016 WL 1532220, at *5 (C.D. Cal. Apr. 15, 2016). And because "[c]osts not related to computer impairment or computer damages are not compensable under the CFAA," claims just like Andrews'—such as "lost revenues" ultimately stemming from data "transferred … to a competitor without [the plaintiff's] authorization" do not qualify under the statute. *SKF USA, Inc.* v. *Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009); *see also, e.g.*, *Farmers Ins. Exch.* v. *Steele Ins. Agency, Inc.*, 2013 WL 3872950, at *21 (E.D. Cal. July 25, 2013) (no loss where plaintiffs sought "lost present and future business revenue" from alleged misappropriation of policyholder data); *U.S. Gypsum Co.* v. *Lafarge N. Am. Inc.*, 670 F. Supp. 2d 737, 743–44 (N.D. Ill. 2009) (similar); *New Show Studios LLC* v. *Needle*, 2014 WL 2988271, at *7 (C.D. Cal. June 30, 2014) (similar). Because Andrews' proposed claim was doomed to fail, the district court did not abuse its discretion in denying leave.

B. Andrews' Counterarguments Are Unavailing

Andrews does not address the textual arguments set forth above. Instead, he contends that this Court already held "obtain[ing] valuable information about … marketing practices" qualifies as a "loss" in *Creative Computing* v. *Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004). Br. 54–55. *Creative Computing* said nothing of the sort. There, Getloaded's officers hacked into Creative Computing's load-matching website to examine the source code for one of its most profitable features and bribed a Creative Computing employee to access and download thousands of confidential customer files. *See* 386 F.3d at 932. On appeal, this Court held that the statute did not "require proof of $5,000 of damage or loss from a single unauthorized access," but rather that "the $5,000 floor applies to how much damage or loss there is to the victim over a one-year period." *Id.* at 934. It also held that "loss of business and business goodwill" qualified as "economic damages" under a provision in the CFAA limiting claims like Creative Computing's to such damages. *Id.* at 935.

Neither holding has anything to do with this case. *Creative Computing* did not address what *counts* as a loss; it simply held that plaintiffs need not show any particular intrusion cost them $5,000 in losses. There was no reason to address whether Creative Computing's alleged loss of business and business goodwill qualified as a loss; as Creative Computing explained without contradiction, it spent more than $5,000 in remedial measures, allowing it to relegate its argument that lost profits sufficed to a sentence in a footnote. *See* 2003 WL 22340437, § I.E (July 14, 2003) (Creative

Computing's brief). And *Creative Computing*'s holding about economic damages is even further afield. A different provision of the CFAA limits recovery for certain plaintiffs to "economic damages," *see* 18 U.S.C. § 1030(g), a term which has long included "lost profits and loss of good will or business reputation," 386 F.3d at 935 & n.19. Whatever "economic damages" means, however, "loss" is a specifically defined term in the statute, one that cannot include Andrews' supposed missed marketing opportunities without making a hash of Congress's wording and transforming the CFAA into a misappropriation statute. *Creative Computing* does not compel that incorrect result.

Andrews seeks additional support from two out-of-circuit district court cases. *See* Br. 55. One of those cases simply asserts—with no reasoning at all, let alone reasoning responding to the points above—that a party may adequately plead loss by alleging loss of revenue without any interruption of service. *See CoStar Realty Info., Inc.* v. *Field*, 612 F. Supp. 2d 660, 675 (D. Md. 2009). Andrews' other cited decision addressed whether the CFAA allowed for "recovery of the physical damage to Plaintiff's computer system only." *Ervin & Smith Advert. & Pub. Relations, Inc.* v. *Ervin*, 2009 WL 249998, at *8 (D. Neb. Feb. 3, 2009). To the extent it even suggested that claims like Andrews' could proceed, it, too provided no reasoning to support that atextual, far-reaching conclusion.

C. Even If Missed Marketing Opportunities Qualified as "Loss" Under the CFAA, Andrews Could Not Plead a Plausible Claim

Even if the district court and Sirius XM were wrong about the meaning of "loss" under the CFAA, Andrews' claim would still be futile, because he cannot plausibly allege $5,000 in missed marketing opportunities. The Third Circuit's decision in *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015), shows why. There, plaintiffs alleged that they had sufficiently pleaded loss under the CFAA because they alleged that Google's deceptively placed browser cookies "depriv[ed] the[m] of their own ability to sell their internet usage information." *Id.* at 148–49. Without addressing whether this alleged loss qualifies as a "loss" under the CFAA, the Third Circuit held that the plaintiffs had not adequately pleaded their case. "They allege[d] no facts suggesting that they ever participated or intended to participate in the market they identify," nor did they "allege that they sought to monetize information about their internet usage," or that they "ever stored their information with a future sale in mind." *Id.* at 149. As a result, the plaintiffs alleged "no revenue" that they actually lost. *Id.*; *see also, e.g.*, *Del Vecchio* v. *Amazon.com, Inc.*, 2012 WL 1997697, at *4 & n.5 (W.D. Wash. June 1, 2012) (plaintiffs failed to adequately plead loss even assuming missed marketing opportunities count because they did not "allege that they attempted to sell their 'private information' … and were rebuffed because [the defendant] had already sold or publicized that information" and had not alleged that the information was

"economically exploitable by Plaintiffs and Class Members," but rather that it was "valuable" only to Amazon).

Andrews could not amend his complaint to meet these standards. His proposed complaint claims that "at least 100 persons" lost out on their $100 chance to sell a "hot lead"—their contact information and the fact that they bought a car equipped with a Sirius XM radio—to Sirius XM. ER 93–94 (Proposed Amended Compl. ¶¶ 35–37). Those proposed allegations are already implausible on their face. Andrews provides no factual details at all to support his claim that a "hot lead" is worth $100, and no company would ever pay anywhere near $50 each—the amount Andrews must plead to reach the $5,000 threshold—for information that *might* help it sell *one* subscription worth between $10.99 and $20.99 a month. *See* https://goo.gl/rsgGAK (pricing for Sirius XM's most popular packages). More importantly, Andrews does not propose to allege any of the facts required in *In re Google*: that there is an existing market in which Sirius XM pays car buyers for their information; that he tried, would have tried, or will try to participate in that market; and that his fellow class members would have made such efforts as well. Even if the lost opportunity to sell his information to Sirius XM qualified as a "loss" under the CFAA's anti-hacking provisions, Andrews has not proposed allegations that would "nudge[] [his] claim[] across the line from conceivable to plausible." *Bell Atl. Corp.* v. *Twombly*, 550 U.S. 544, 570 (2007).

CONCLUSION

The judgment below should be affirmed.

STATEMENT WITH RESPECT TO ORAL ARGUMENT

Sirius XM respectfully requests oral argument. While the district court's decision is clearly correct, this case involves several distinct issues and a detailed set of facts. Sirius XM believes that oral argument would aid the Court in its resolution of this appeal.

STATEMENT OF RELATED CASES

Sirius XM is not aware of any related cases as defined by Ninth Circuit Rule 28-2.6.

Dated: July 11, 2018

Respectfully submitted,

/s/ Shay Dvoretzky

Shay Dvoretzky
Jeffrey R. Johnson
JONES DAY
51 Louisiana Ave., N.W.
Washington D.C. 20001
Tel: (202) 879-3939
Fax: (202) 626-1700

Thomas Demitrack
JONES DAY
901 Lakeside Ave.
Cleveland, OH 44114
Tel: (216) 586-3939
Fax: (216) 579-0212

Lee A. Armstrong
JONES DAY
250 Vesey Street
New York, New York
Tel: (212) 326-3939
Fax: (212) 755-7306

Counsel for Appellee Sirius XM Radio Inc.

Form 8. Certificate of Compliance Pursuant to 9th Circuit Rules 28.1-1(f), 29-2(c)(2) and (3), 32-1, 32-2 or 32-4 for Case Number 18-55169

Note: This form must be signed by the attorney or unrepresented litigant *and attached to the end of the brief.*

I certify that (*check appropriate option*):

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 28.1-1.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☒ This brief complies with the length limits permitted by Ninth Circuit Rule 32-1.
The brief is [13,027] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 32-2(b).
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable, and is filed by (1) ☐ separately represented parties; (2) ☐ a party or parties filing a single brief in response to multiple briefs; or (3) ☐ a party or parties filing a single brief in response to a longer joint brief filed under Rule 32-2(b). The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the longer length limit authorized by court order dated [ ]
The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable.

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 32-2 (a) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32 (f), if applicable. The brief's type size and type face comply with Fed. R .App. P. 32(a)(5) and (6).

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 29-2 (c)(2) or (3) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits set forth at Ninth Circuit Rule 32-4.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Signature of Attorney or Unrepresented Litigant: s/ Shay Dvoretzky

Date: 07/11/2018

("s/" plus typed name is acceptable for electronically-filed documents)

CERTIFICATE OF SERVICE

I certify that on July 11, 2018, the foregoing was electronically filed with the United States Court of Appeals for the Ninth Circuit using the CM/ECF system. All parties have consented to receive electronic service and will be served by the ECF system.

Dated: July 11, 2018

/*s*/ Shay Dvoretzky

Counsel for Appellee Sirius XM Radio Inc.